UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/770,397	01/29/2001	Susumu Senshu	202442US6	6175

22850 7590 05/02/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
05/02/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	09/770,397	SENSHU, SUSUMU	
	Examiner	Art Unit	
	BEEMNET W. DADA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 29, 2008 has been entered. Claims 1, 6, 10, 15, 19 and 22 have been amended and new claim 26 has been added. Claims 1-26 are pending.

Response to Arguments

Applicant's arguments filed on February 22, 2008 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kato et al (6,301,663) in view of Katoh (2002/0073037) further in view of the article by Kaplan ("IBM Cryptolopes™, SuperDistribution and Digital Rights Management") and further in view of Tsukidate US 2004/0081426 A1.

In reference to claims 1, 6, 10 and 26, Kato discloses a method and system for protecting against unauthorized copy of multimedia (abstract). The method comprises the steps of: Kato further discloses encrypting data identification information of the digital data (column 6 lines 20-24). The Disc key corresponds to the recording medium ID in encryption of data in the form of audio data, which contains the watermark (column 16 lines 15-20), which contains a master key. The Disc key further corresponds to the medium ID since the key identifies the disk in that it is a key belonging to the disk. The watermark contains the master key (column 9 lines 44-47). Therefore the master key (write identification information) is encrypted by the disk key.

Although Kato discloses the use of a disk key (recording medium ID), Kato does not disclose obtaining a recording medium ID associated with the recording medium. Furthermore Kato does not disclose generating independent write identification information for each recording operation of the digital data. Although Kato discloses the use of a disk key to encrypt information, Kato does not disclose encrypting data identification information of the digital data and data control information by the use of the write identification information and encrypting the write identification information by use of the recording medium ID.

Katoh discloses a system and method for controlling copy generation of digital data stored in recording media to protect the data from unauthorized copying (abstract). In the system disclosed by Katoh, there exists a disc ID (page 2 paragraph 0022) and a means to detect and therefore obtain the ID (part 214 Fig. 2 in combination with page 2 paragraph 0024). Katoh further teaches generating independent write identification for every recording operation performed on the digital data (page 2 paragraphs 0020-0022).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have a disc ID and a method to obtain the disc ID and generating independent write identification for every recording operation performed on the digital data as in Katoh in the

system of Kato. One of ordinary skill in the art would have been motivated to do this because the disc ID is useful information for controlling copy control information.

However Katoh does not disclose encrypting the write identification information by use of the recording medium ID; and recording at least the encrypted data identification information and data control information to the recording medium.

Kaplan discloses generating independent write identification information for each recording operation of the digital data (Fingerprinting/watermarking instructions/specifications paragraph 4 page 4 and page 5 paragraph 1); the crytolope can add individualized fingerprints and the identify the licensee or purchaser of each authorized or licensed copy. The cryptolope encrypts data identification information of the digital data and data control information (Fig. 1 Encrypted Fingerprint and watermark instructions) by use of the write identification information (master key). Kaplan further discloses recording at least the encrypted data identification information and data control information to the recording medium (SuperDistribution page 2). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the encryption key as in the Cryptolopes of Kaplan in the system of Kato using the disk key of Kato. One of ordinary skill in the art would have been motivated to do this because this means that royalty/licensing clearing centers do not have to maintain a database of all documents keys, instead, each clearing center maintains a small database of master keys.

The combination of Kato, Katoh and Kaplan is silent on unique recording medium ID recorded on a predetermined region of the recording medium. However, Tsukidate teaches a unique recording medium ID corresponding to the recording medium and the medium ID pre-recorded on a predetermined region of the recording medium [see page 8, claim 14]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to

employ the teachings of Tsukidate within the combination of Kato, Katoh and Kaplan in order to further enhance the security of the system.

In reference to claims 2, 7, and 11, wherein the digital data is encrypted by the data identification information, and the encrypted digital data is recorded to the recording medium along with the encrypted data identification information and data control information (column 7 lines 34-36).

In reference to claims 3, 8, and 12, wherein the data control information includes copy control information for the digital data (column 6 line 66 to column 7 line 1).

In reference to claims 4, 9, and 13, wherein the encrypted data identification information and data control information, and the write identification information (column 10 lines 48-52) are encrypted by the use of recording medium unique to the recording medium and recorded to the recording medium (column 6 lines 1-42).

In reference to claims 5 and 14, wherein a data processing unit for encrypting the data identification information and data control information and a data recording unit for recording data to the recording medium are mounted separately, and the write identification information is generated at the data recording unit, and the generated write identification information is encrypted and transmitted to the data processing unit (Fig. 1).

Claims 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kato et al (6,301,663) in view of the article by Kaplan ("IBM Cryptolopes™, SuperDistribution and Digital Rights Management") and further in view of Tsukidate US 2004/0081426 A1.

In reference to claim 15, 19, and 22, Kato discloses a method and system for protecting against unauthorized copy of multimedia (abstract) comprising the steps of: reproducing encrypted data identification information and write identification information, which are encrypted by the use of recording medium identification information from the recording medium (Fig. 2 part S13 in combination with column 5 lines 57-62); decrypting the encrypted data identification information and data by the use of the write identification information, and taking out the data identification information of the digital data and data control information (Fig. 2 part S13 and S16 in combination with column 7 line 66 to column 8 line 6).

Although Kato discloses recording the copy control and the encryption of the disc key, therefore the potential to store and encrypt the copy control, Kato does not expressly disclose encrypting data control information by the use of the write identification information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the copy control in the system of Kato. One of ordinary skill in the art would have been motivated to do this because encryption discourages fraud and increases the security of digital data.

Kato does not disclose obtaining a recording medium ID associated with the recording medium; and encrypting the write identification information by use of the recording medium ID. Kaplan discloses a system that obtaining a master key to encrypt the keys of the cryptolope (page 3; Key records; paragraph 1). The master key corresponds to the recording medium id. The master key is obtained from the clearing center (page 4 paragraph 2). The identification

information is encrypted using the recording medium ID (page 3; Key records; paragraph 1). The document keys correspond to the identification information; these are encrypted using the master key (recording medium ID). The master key is unique to the particular collection of documents (page 9 paragraph 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the encryption key as in the Cryptolopes of Kaplan in the system of Kato. One of ordinary skill in the art would have been motivated to do this because this means that royalty/licensing clearing centers do not have to maintain a database of all documents keys, instead, each clearing center maintains a small database of master keys.

The combination of Kato and Kaplan is silent on unique recording medium ID recorded on a predetermined region of a recording medium. However, Tsukidate teaches a unique recording medium ID corresponding to the recording medium and the medium ID pre-recorded on a predetermined region of the recording medium [see page 8, claim 14]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Tsukidate within the combination of Kato and Kaplan in order to further enhance the security of the system.

In reference to claims 16, 20 and 23, wherein the digital data is encrypted by the data identification information and recorded to the recording medium, and the encrypted digital data is reproduced from the recording medium along with the encrypted data identification information and data control information, and the write identification information (column 7 lines 34-36).

In reference to claims 17, 21, and 24, wherein the encrypted data identification information and data control information, and the write identification information (column 10 lines 48-52) are encrypted by the use of the recording medium identification information peculiar to the recording medium (column 6 lines 1-42) and recorded to the recording medium, and the recording medium identification information is reproduced from the recording medium, and the data encrypted by the recording medium identification information are decrypted by the use of the recording medium identification information, and the encrypted data identification information and data control information, and the write identification information are taken out (Fig. 1).

In reference to claim 18, wherein a data processing unit for encrypting the data identification information and data control information and a data recording unit for recording data to the recording medium are mounted separately, and the write identification information is generated at the data recording unit, and the generated write identification information is encrypted and transmitted to the data processing unit (Fig. 1).

In reference to claim 25, wherein said generating step includes generating the write identification information with a random number generator (part 113 Fig. 10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/

Art Unit 2135

April 23, 2008